

Zugang per ReverseProxy

Die Konfiguration eines [ReverseProxy](#) und der Einsatz von [Let's Encrypt](#) werden in einem separaten Buch aufgegriffen.

Hier an dieser Stelle daher nur eine kurze Zusammenfassung.

Auf dem [ReverseProxy](#) (hier ein [Apache 2.4](#) Web-Server) wird für dieses Beispiel folgende Konfiguration (bspw. als `/etc/apache2/sites-enabled/stirling.conf`) angelegt:

```
<VirtualHost subdomain.schubert.si:80>
    ServerAdmin webmaster@schubert.si
    ServerName subdomain.schubert.si
    ServerSignature Off
    DocumentRoot /var/www/html/stirling
    RewriteEngine on
    RewriteCond %{SERVER_NAME} =subdomain.schubert.si
    RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,NE,R=permanent]
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Das unter *DocumentRoot* angegebene Verzeichnis ist nur ein Dummy mit einer leeren *index.html*-Datei.

Gebraucht wird das leere Verzeichnis nur für den Einsatz des Certbot von [Let's Encrypt](#).

Auch wenn es zunächst so aussehen mag:

Es wird kein Dienst unter Port 80 (unverschlüsseltes HTTP) angeboten, sondern per Rewrite wird jeglicher Aufruf von HTTP auf HTTPS umgeschrieben.

Analog zur Konfiguration für Anfragen an Port 80 gibt es eine weitere Konfiguration (bspw. als `/etc/apache2/sites-enabled/stirling-le-ssl.conf`) oder als weiteren Abschnitt in der ersten Konfigurationsdatei, um eben die Anfragen an Port 443 (HTTPS) zu beantworten:

```
<IfModule mod_ssl.c>
<VirtualHost subdomain.schubert.si:443>
    ServerAdmin webmaster@schubert.si
    ServerName subdomain.schubert.si
    ServerSignature Off
```

```
ProxyPreserveHost On
ProxyPass / http://192.168.1.11:8080/
ProxyPassReverse / http://192.168.1.11:8080/
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
SSLCertificateFile /etc/letsencrypt/live/subdomain.schubert.si/fullchain.pem
SSLCertificateKeyFile /etc/letsencrypt/live/subdomain.schubert.si/privkey.pem
Include /etc/letsencrypt/options-ssl-apache.conf
</VirtualHost>
</IfModule>
```

Hinter *ProxyPass...* wird die (interne) IPv4-Adresse der virtuellen Maschine angegeben, die Stirling-PDF bereitstellt.

Dafür müssen sich natürlich sowohl die VM mit dem [ReverseProxy](#) als auch die VM mit Stirling-PDF im gleichen Subnetz befinden.

Sollte der [ReverseProxy](#) auf der gleichen Maschine laufen wie Stirling-PDF selbst, wird stattdessen localhost (<http://localhost:8080> oder <http://127.0.0.1:8080>) verwendet

Nach Anlage der Konfiguration muss diese Apache noch mittels `systemctl reload apache2` bekannt gemacht werden.

Somit kann Stirling-PDF per HTTPS unter dem Standard-Port 443 anstatt über eine unverschlüsselte HTTP-Verbindung genutzt werden.

Revision #2

Created 11 April 2024 13:55:41 by Rene Schubert

Updated 12 April 2024 05:51:19 by Rene Schubert